Typologie de la fraude

NOËL PONS
Conseiller au Service central de prévention de la corruption, auditeur interne certifié et inspecteur des impôts

Quels sont aujourd'hui les risques de fraudes les plus fréquentes ? Il existe classiquement les risques de fraudes internes et externes telles que l'usage de faux documents, mais il ne faut pas non plus négliger les risques relatifs au support informatique et à l'internet ainsi que ceux liés aux placements boursiers et aux manipulations des bilans.

Il y a vingt ans, la fraude dans les banques était relativement simple à identifier : l'environnement était clos, les flux, somme toute, limités et les opérations complexes réalisées dans un cadre compréhensible par tous.

Depuis, le changement radical de l'environnement, lié à la mondialisation, a généré des faiblesses notables :

– la désintermédiation des activités ;
– un entrelacs de liaisons directes et indirectes entre des acteurs dont une bonne partie n'est pas des banquiers ;
– l'utilisation de modèles mathématiques qui a, au sens propre, retiré le contrôle du cadre habituel dans certains domaines ;
– de façon concomitante, les banques se sont mises à exercer d'autres métiers ; elles sont toutes entrées dans l'ère Internet.

Cette évolution est accompagnée d'une augmentation des flux, des échanges et d'une dérégulation générale. La complexité des opérations a rendu certains contrôles quasiment impossibles alors que d'autres ont été remisés au second plan. En fait, l'augmentation constante du nombre de produits a camouflé les fraudes qui sont devenues des pertes collatérales acceptables.

Aujourd'hui, il est possible de dresser un inventaire des fraudes les plus fréquentes et de le structurer ainsi :

– les risques de fraude interne, celui toujours présent du conflit d'intérêt (*ce point est détaillé dans le second texte de Noël Pons p. 14*) ;
– les risques de fraude externe ;
– les risques relatifs au support informatique et à Internet qui recouvre les précédents, mais sous une forme spécifique ;
– enfin, les risques liés aux placements boursiers et aux manipulations des bilans.

Cette analyse, il faut le préciser, est effectuée par un non-banquier et à l'extérieur du système. Elle est donc susceptible de surprendre du fait de la terminologie utilisée.

Risques internes pour les banques

Les risques internes sont liés au comportement du personnel. Le fraudeur est souvent un collaborateur. Il connaît bien le secteur et maîtrise les opportunités de camouflage des manipulations mises en place. Par exemple, il existe un certain nombre de fraudes sur les crédits :

– prorogation des échéances, le ratio de recouvrement semble correct alors que les prêts sont irrécouvrables ;
– ouverture illégale des comptes, une fois les instruments de paiement obtenus, ils sont rendus débiteurs et passés en pertes ;
– création dans les comptes de faux titulaires de crédits. On constate toujours ce type de manipulation dans les périodes fastes ;
– utilisation personnelle des prêts laissés libres par des remboursements anticipés. Cette procédure, bien connue, dite "des prêts d'occasion" est pertinente lorsque le coût du crédit augmente ;
– utilisation des dossiers péri-

Noël Pons a publié plusieurs ouvrages :
• "Audit et fraudes", éditions Ifaci, Paris 2004, avec François Vidaux
• "Cols blancs et mains sales-économie criminelle mode d'emploi", Odile Jacob, Paris 2006
• "Arnaques – le manuel anti-fraudes", CNRS éditions, Paris 2009.

més ou dormants pour camoufler des détournements effectifs. Des fausses données sont introduites dans les dossiers "morts", puis les programmes sont modifiés de manière à couvrir techniquement les détournements réalisés ;
– décalage de la clôture d'un compte client qui en avait fait la demande et utilisation à d'autres fins ;
– autorisation de découvert fictive ;
– pillage des comptes immobiles.

Ces diverses manipulations s'accompagnent souvent du traitement des données informatiques des comptes, ce qui permet de camoufler l'opération et la perpétue.

Enfin, il existe de nombreux autres types de risques concernant la gestion de la caisse et des divers comptes personnels des clients, qui constituent le fonds de l'activité frauduleuse des salariés des banques.

Risques externes pour les banques

L'utilisation de faux documents touche particulièrement le secteur bancaire ainsi que celui des assurances. Il constitue le support essentiel des fraudes externes et concerne à la fois les individus et les sociétés. Ce type de fraude, qui a cru de manière exponentielle, nécessite des explications complémentaires.

L'usage de faux concerne l'ensemble des clients des banques. Les particuliers peuvent par ce moyen ouvrir des comptes, obtenir des prêts, disposer de cartes de crédit. En France, un escroc organisé peut disposer, en jouant sur plusieurs banques, de 30 000 euros environ. Ces comptes sont utilisables pour frauder, mais aussi pour blanchir. Dans ce cas, le flux est entrant au lieu d'être sortant pour les fraudes. L'utilisation de ces faux se décline de plusieurs manières.

▮ Il peut s'agir d'un faux document intégré dans un dossier (les crédits Alt A sont désormais célèbres) qui accompagne une situation relevant de la fraude, mais qui ne sera pas forcément identifiée. Seuls des événements extérieurs forts et conjoints peuvent causer des pertes immédiatement visibles, la crise des crédits *subprime* en étant l'exemple frappant. En fait, ces documents falsifiés permettent de gagner du temps sur le contrôle.

▮ Il peut s'agir de documents manipulés par une personne isolée avec un scanner et une photocopieuse ou un logiciel comptable. Elles restent cependant risquées car aisément identifiables.

▮ Enfin, s'agissant d'un "kit", la situation est alors toute autre. C'est un ensemble de documents, en général établis par des faussaires liés à la grande criminalité, qui sont vendus et dont la qualité leur confère une certaine sécurité d'utilisation.

Le problème du salami

■ Les fraudes liées au système d'informations, si ce dernier n'est pas utilisé convenablement, peuvent être dévastatrices pour l'ensemble des activités. Les fraudes relevées sont le plus souvent constituées par une accumulation de petits détournements considérés unitairement comme non significatifs. Elles entrent dans la typologie des manipulations appelées "à effet levier" [1]. On les différencie des fraudes dans lesquelles les détournements sont plus importants unitairement et qui nécessitent des complicités ou des informations internes. Les montages touchent obligatoirement le système informatique dont elles utilisent une faille, en général un accès indu. Il peut s'agir d'un comptable qui crée un faux fournisseur ou qui manipule un rapprochement bancaire, d'un informaticien qui utilise une faille dans une base de données à partir d'une porte dérobée (*back door*) non documentée… Déceler ce type de fraude exige l'utilisation d'outils de détection spécifiques car elle repose sur un dysfonctionnement du contrôle interne. L'usurpation de l'identité d'un utilisateur, l'accès à des données non légitimes, le forçage de transactions non autorisées, la modification ou la suppression directe des données constituent les manipulations les plus courantes.

■ Un exemple de détournement à effet levier doit être exposé : il s'agit d'un montage célèbre couramment appelé le "salami" et découvert au cours des années 1960. En fraude informatique, le montage permet de récupérer de très petites sommes, parfois en dessous du centime, mais qui, cumulées, deviennent un gain intéressant pour un individu.

■ Le quotidien *Les Échos* relatait, à l'occasion d'un colloque sur la fraude fin 2007 : "*La fraude à la paye – Dans une entreprise de taille moyenne ou grande, l'employé du service paye crée un programme spécifique dans la base. C'est la technique dite du "salami" : il détourne de toutes petites sommes – par exemple quelques centimes après la virgule – prélevées sur chaque feuille de paye mensuelle. Qui regarde son bulletin de paye à la virgule près ? Personne…*"

■ Dans ce cas, le fraudeur est souvent programmeur. Même en ne lésant que très faiblement les clients, le bénéfice est significatif pour une personne physique qui aurait accès aux comptes. Le gain grimpe très vite en tronquant un chiffre de plus élevé pour atteindre un montant énorme. La technique du salami va consister à détourner toutes ces petites sommes et les virer sur un ou plusieurs comptes intrus. Au cours du traitement, le fraudeur a la possibilité de générer la reprise du calcul correct quand le cumul a atteint un montant "suffisant" ou qu'il sait être hors du seuil de déclenchement d'un contrôle.

1. Il s'agit de détournements faibles unitairement, mais qui du fait du caractère systématique des opérations informatisées, créent des détournements importants et récurrents.

Les entreprises peuvent générer des dossiers voire créer d'autres entités totalement fictives qui permettront d'asseoir un montage frauduleux ou de blanchiment.

Ainsi, dans le premier secteur (faux documents), les dossiers sont souvent complets et ils constituent pour le fraudeur une source de revenus non négligeables.

« Il existe de nombreux types de risques concernant la gestion de la caisse et des divers comptes personnels des clients, qui constituent le fonds de l'activité frauduleuse des salariés des banques. »

Lorsque les services de contrôle auront clôturé leurs analyses, les manipulations suivantes seront probablement identifiées :

– faux documents intégrés dans les dossiers de demandes de prêts afin de mieux faire accepter l'opération (faux revenus, faux noms, fausse qualité) ;
– dossiers falsifiés permettant aux proches des courtiers de bénéficier de ces prêts ;
– fausses demandes permettant à l'intermédiaire de détourner à titre personnel ces sommes (une escroquerie classique au prêteur) ;
– existence de structures pyramidales dédiées à la recherche de "clients" et à la remontée des fonds se développant souvent à partir de sociétés sans fonds propres, elles-mêmes financées par les opérations générant des bulles spéculatives.

Ces montages sont organisés entre proches, ce qui facilite encore l'enrichissement personnel. L'un des montages les plus classiques à ce jour reste l'utilisation de faux transferts comportant des ordres de virement dont la signature est parfaite pour des destinations improbables. Dans ce cas, le seul moyen de contrôle est le contre-appel qui touche surtout des virements "papier". L'informatique a, en partie, encadré ce risque, il reste néanmoins très usité dans des pays pour peu qu'ils soient un peu moins surveillés.

Un lourd vecteur de fraudes est organisé autour de sociétés écrans et de manipulations commerciales. La liste est longue :

– les effets dits "de famille", tirés entre les sociétés d'un même groupe et qui présentent un risque important lorsque la trésorerie du groupe est défaillante ;
– les effets "creux" qui ne correspondent à aucune transaction matérialisée ;
– les effets "fictifs" tirés sur un tiers qui existe, mais dont il n'est pas débiteur, le tiers étant donc instrumentalisé à son insu ;
– les effets de complaisance destinés à procurer un crédit non justifié à une entreprise ;
– l'échange financier non solvable et les prêts irrécouvrables sont échangés entre deux organisations et sont comptabilisés dans chacune des structures comme de nouveaux prêts ;
– les prêts croisés, quand un emprunt est obtenu par un responsable des prêts d'une banque auprès d'une autre banque, le responsable de la seconde organisation obtenant un prêt similaire de la première ;
– les achats immobiliers, par exemple, au moyen de prêts eux-mêmes revendus à un autre acheteur disposant lui-même d'un prêt de même nature ;
– l'ouverture d'un compte client fictif ;
– la cavalerie de chèques qui était qualifiée par un spécialiste des fraudes bancaires comme "*l'un des quatre cavaliers de l'apocalypse*" et qui nécessite une complicité interne.

Ces opérations supposent la falsification délibérée des documents tels que les garanties et autres justificatifs, parfois de manipulations des logiciels de gestion ou comptables.

La crise des crédits *subprime* a mis en évidence plusieurs risques qui ont surpris de nombreux analystes : les courtiers ont démarché, pour le compte des établissements prêteurs, les "emprunteurs", appartenant le plus souvent à des communautés pauvres issues de l'immigration mexicaine ou africaine. Chacune des ventes, pour les intermédiaires comme pour les structures qui prêtaient les fonds, générait des bonus considérables calculés sur les fonds "placés". Leur intérêt immédiat était donc de vendre un maximum de "contrats", les bonus étant majorés pour les placements les plus risqués.

Les risques informatiques pour les banques

Cette typologie affecte à la fois la fraude externe et la fraude interne. Comme pour toutes les organisations, la fraude informatique recouvre la fraude réalisée par des informaticiens dont le décèlement précoce est quasiment impossible du fait de sa matérialisation située au-dessous du niveau du contrôle interne.

La fraude informatique externe relève plutôt des services de sécurité chargés de protéger les actifs de l'entreprise, en particulier des intrusions extérieures. Autre élément, le vol des codes Internet des clients dans leur boîte à lettres ou courriel. Le service ne constate rien car le contrat est validé. Internet pose quelques problèmes complémentaires car dans ce cas, on ne connaît pas personnellement le client.

Dans le secteur bancaire, tout peut être de la fraude informatique puisque tout passe par l'informatique. Nous ne citerons ici que les attaques par les virus qui peuvent porter sur les fichiers de sauvegarde ou sur les programmes sources :

– casse des codes d'accès d'un serveur boursier et modification artificielle du taux, ce qui a entraîné une baisse mécanique du cours et permis à un complice d'acheter des actions à un niveau très bas ;
– simulation de baisse des cours sur un serveur, rachat sur des comptes-clients fictifs, revente au moment où il remonte et effacement des comptes ;
– suppression de certains contrôles sur une chaîne suivie d'opérations frauduleuses sur les comptes.

La fraude interne informatique existe également. On citera les détournements des employés qui utilisent

les mots de passe des clients. La mécanique consiste à augmenter le plafond de crédit en interne puis le détournement de la différence est effectué à partir d'un simple distributeur de billets.

Le problème du support informatique se pose souvent. Un logiciel, installé depuis longtemps et maintes fois adapté, ne permettra pas de traiter rapidement les alertes ou ne réalisera des contrôles que sur les soldes, par exemple. En fait, nombreux sont ceux qui connaissent les codes des applications comme ceux des utilisateurs car la gestion des accès est perméable.

Quelques autres fraudes internes peuvent être particulièrement lourdes pour les banques ? Il s'agit de fraudes sur les virements à partir de transactions licites, de fraudes sur les taux des devises, ainsi que des faux virements sur les vrais comptes de complices.

L'élargissement des zones de risques liées directement aux systèmes d'information résulte :

– du nombre d'opérations effectuées ;
– de l'exigence de rapidité des traitements ;
– de failles, en apparence anodines, existantes dans les systèmes ;
– de la dématérialisation des documents qui aggravent les risques de fraudes en diminuant considérablement le temps de réaction lorsque des remontées de listes d'erreurs existent ; dans le cas contraire, le risque devient immense ;
– du transfert électronique de données, outil remarquable qui permet l'échange de données immédiat mais qui pose une vraie problématique : en effet, un tel système n'est sûr que dans le cas où la sécurité présente le même degré de protection chez les deux partenaires, où une faille existant chez l'un est automatiquement importée chez l'autre ;
– de la multiplication des défaillances le plus souvent corrigées sans qu'une analyse fraude aie jamais été effectuée.

Ces risques inhérents au support informatique doivent être mis en balance avec la nécessaire utilisation du système. Une prévention des risques à 100 % correspond à un blocage du dispositif ; à 90 %, il est lent et peu réactif et à 80 %, il fonctionne correctement, mais des failles sont ouvertes. Les responsables doivent choisir entre Charybde et Scylla et disposer d'une cartographie des risques très pertinente pour "embarquer" des contrôles spécifiques des points identifiés comme présentant un risque conséquent.

Il existe également les fraudes implantées sur le support informatique. Il s'agit de montages utilisés depuis longtemps. Ce type de fraudes nécessite un forçage des comptes (des données qui ne devraient pas se trouver dans le système informatique y sont intégrées du fait de l'existence d'une faille dans la séparation des fonctions), mais sont correctement identifiables par des analyses des fichiers développées par des logiciels d'audit.

À titre d'exemple, l'une des fraudes les plus répandues qui consiste à créer une fausse facture et à l'intégrer par forçage dans le circuit comptable (cela suppose des manipulations manuelles : copiage, scannage ou création d'une fausse pièce justificative…) a quelque peu évolué.

Depuis l'avènement informatique la recherche peut être réalisée en trois temps :

– une revue des habilitations informatiques atypiques ou intruses identifiables par des traitements de masse permet d'identifier les intervenants ;
– une revue des comptes bancaires pour identifier les comptes intrus qui bénéficient des versements ;
– une analyse du cheminement des opérations au travers des logiciels utilisés.

La difficulté apparente du support informatique permet à celui qui le maîtrise d'effectuer des recherches qu'il n'aurait pu mener à bien manuellement. Mais ces recherches, bien qu'exhaustives, ne mettent en évidence que les montages grossiers.

Les attaques par Internet

Les agressions externes par Internet sont devenues monnaie courante. Internet n'a pas créé de fraudes réellement nouvelles, mais il permet, facilite et amplifie la propagation des fraudes existantes. Internet est criminogène du fait de sa dématérialisation et de l'impunité de l'acte qu'il procure. Avec Internet s'est créé un nouvel espace social, complètement immatériel. La seule réalité est constituée par les espèces ou les fonds détournés. Il y a aussi le virus, logiciel qui parasite un matériel à l'insu de l'utilisateur. Après activation, il utilise les ressources des fichiers pour se propager. Dans certaines organisations, le problème est devenu tellement sensible que son traitement a été directement rattaché à la direction générale.

La cartographie des risques, pour aussi variée qu'elle soit, est ordonnée autour de trois points :

– le déni de service : la lecture des documents commerciaux et personnels envoyés par Internet est impossible ou il est impossible de travailler ;
– le pillage des données propres au cœur de métier ;
– le dernier avatar identifié est appelé *pharming*, sorte de *racket* qui consiste pour un *hacker* à s'emparer des fichiers essentiels pour une entreprise, de l'encoder, puis de demander une rémunération pour le rendre à nouveau utilisable. Une fois encore, c'est la grande criminalité qui a conçu et exécuté ce montage.

« Quelques autres fraudes internes peuvent être particulièrement lourdes pour les banques ? Il s'agit de fraudes sur les virements à partir de transactions licites, de fraudes sur les taux des devises, ainsi que des faux virements sur les vrais comptes de complices. »

Le service de sécurité a la charge de ce type de protection. Cependant, cette activité devrait être élargie à d'autres spécialistes plus informés des fraudes.

Enfin, les risques informatiques sont aussi caractérisés par les fraudes sur les taux de devises, avec manipulation des tables : par exemple, des virements depuis une banque anglaise vers une société commerciale russe, en contrepartie de faux achats de diamants. Cela se traduit souvent par des virements illicites avec des codes d'authentification exacts.

Manipulations boursières

Outre la problématique bien connue du *trading*, il existe un large éventail de manipulations dans ce domaine.

- Des gains qui auraient dû rester affectés sur ceux de leurs propriétaires (vérifications effectuées sur des *mutual funds* par la SEC) sont détournés vers les comptes des dirigeants. L'énorme quantité d'opérations rend les contrôles fragiles. Les virements de ce type constatés au crédit du compte d'un *manager* d'un fonds devraient faire l'objet d'une déclaration de soupçon.
- Des dérivés sont utilisés pour prendre des positions "rampantes" sans être identifié ou ne sont pas documentés de manière à ce qu'ils restent camouflés.
- Des ordres importants de clients à la valeur liquidative sont passés après la clôture des marchés. Ce type de manipulation est utilisé par le grand banditisme qui place ses paris après l'arrivée de courses. Ces pratiques dites de *late-trading* pourraient ne pas avoir fait l'objet de contrôles appropriés. C'est une stratégie intéressante en termes de bonus et de chiffre d'affaires.
- Des plus-values obtenues à l'occasion de placements réalisés avec les fonds de clients sont détournés au bénéfice d'autres clients, pour leur compte propre ou encore pour celui de proches. Ces montages sont facilités à l'occasion d'opérations effectuées de gré à gré, donc sans contrepartie officielle, et pendant les périodes où les cours des actions "travaillées" varient beaucoup (à la hausse ou à la baisse).
- Les criminels organisent une "bouilloire" : très ancien montage qui consiste à faire varier par des achats importants et des communications falsifiées les cours d'actions ou de matières premières, de manière purement factice afin d'en tirer un bénéfice lors de la vente (le dernier cas connu est celui de Crown Corporation courant janvier 2009) ;
- Des achats et des ventes sont multipliés (écrêtage) : ces allers-retours maximisent les commissions liées aux opérations. Cette pratique n'est pas illégale, mais le devient lorsque les opérations sont effectuées sur des produits sophistiqués, sur lesquels les clients n'ont pas de lisibilité et que des commissions sont facturées pour des opérations qui n'ont pas eu lieu.
- Des ventes à découvert sont multipliées. Elles permettent de retirer des plus-values lors de la baisse des cours, mais aussi de faire chuter la valeur d'action des sociétés pour les acheter à moindres coûts.

La réussite des montages frauduleux dans les banques, comme ailleurs, réside souvent dans la légèreté du recrutement : l'urgence, le manque de précautions, l'implication forte dans les réseaux locaux sont autant de négligences qui peuvent causer des catastrophes. C'est ainsi que l'on peut suivre une succession d'escroqueries commises par un individu louche qui a tour à tour démissionné de plusieurs banques ou cabinets d'assurances, parfois de manière très expéditive, mais sans qu'aucune plainte n'ait jamais été déposée. Il poursuit alors, un peu à la manière des *serial killers*, ses méfaits dans des structures différentes.

Un autre élément pouvant faciliter la fraude est la carence de mobilité du personnel . Ce n'est pas un hasard si la grande majorité des fraudes internes dites "du comptable" sont découvertes pendant l'absence du titulaire du poste. Le manque de séparation des pouvoirs est aussi un facteur d'insécurité : difficile à mettre en place dans des petites structures, c'est son coût qui est souvent dissuasif dans des structures plus techniques.

Le recrutement des personnes, la culture du "pas de vagues" – en baisse ces temps-ci –, quelques fonctions à risque sont des vecteurs essentiels de la fraude. Certaines fonctions sont plus touchées que d'autres : l'exercice isolé d'une activité, la responsabilité d'une fonction organisée en monopole...

L'un des risques "forts" est représenté par des agents isolés dans de petites agences, pour deux raisons : l'éloignement du contrôle, d'abord, et la quasi-absence de séparation des fonctions. En contrepartie, les détournements sont souvent négligeables au final...

> *« Internet n'a inventé que peu de fraudes réellement nouvelles, mais il permet, facilite, amplifie la propagation des fraudes existantes. Internet est criminogène du fait de sa dématérialisation et de l'impunité de l'acte qu'il procure. »*

Un inventaire incomplet

Mais cette liste de fraudes est loin d'être exhaustive : on trouve les fraudes sur les cartes (fausses cartes à partir de fichiers détournés, faux terminaux de paiement...), sur les opérations commerciales (tirages croisés, fausses traites, cavalerie s'il n'y a pas de complicité...), mais aussi les fraudes à l'assurance, les délits d'initiés. Chacune de ces fraudes pouvant également être interne lorsqu'elle implique un salarié... Les limites sont difficiles à placer. ■